WHAT IS CLAIMED IS:

1. A method for transmitting a message between a sender associated with a first e-mail firewall and a recipient associated with a second e-mail firewall, the method comprising:

   intercepting a message from the sender intended for the recipient;

   searching an encryption directory for an entry associated with the recipient;

   retrieving an encryption key associated with a second firewall, the second firewall associated with the recipient;

   encoding the message with the encryption key of the second e-mail firewall to provide an encrypted message; and

   allowing the message to proceed through the firewall.

2. The method of Claim 1, wherein said encoding the message is by employing an encryption key that is stored locally by the first e-mail firewall.

3. The method of Claim 1, wherein said encoding the message is by employing an encryption key that is retrieved from an external server.

4. The method of Claim 3, wherein retrieving the key from an external server is over a secure communication link.

5. The method of Claim 4, wherein the secure communication link is by employing a locally stored encryption key associated with the external server.

6. A method for receiving a message from a sender associated with a first e-mail firewall, the first e-mail firewall encoding the message by using an encryption key of the second e-mail firewall, comprising:

   intercepting the message by the second e-mail firewall;

   decoding the message with a private key of the second e-mail firewall; and

   allowing the message to proceed through the firewall to the recipient.

7. A method for controlling e-mail message transmission across an e-mail firewall, the e-mail firewall interposed between an internal network and external networks, the method comprising:

   intercepting a message from a sender associated with the internal network to a recipient associated with an external network;

17

filtering the message by examining content associated with the message by employing user-defined content filter conditions of the e-mail firewall; and restricting the transmission of the message in accordance with the results of said filtering.

8. The method of Claim 7, wherein said filtering is by parsing the text of the message in accordance with said filter conditions.

9. The method of Claim 8, wherein said parsing of text is by searching for keywords in the text.

10. The method of Claim 8, wherein said parsing of text is by searching for word patterns in the text.

11. The method of Claim 10, wherein said filter conditions employ Boolean expressions.

12. The method of Claim 7, wherein said filtering conditions include rejecting all executable attachments.

13. The method of Claim 7, wherein said filtering conditions include requiring executable attachments to include digital signatures.

14. The methof Claim 13, further comprising filtering executable attachments by reference to a directory of trusted signatures.

15. The method of Claim 7, wherein said restricting the transmission includes routing the message in accordance with user defined routing policies.